In the Claims:

Please cancel claims 2-25. Please amend claim 1. Please add new claims 27-49. The claims are as follows:

1. (Currently amended) A method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, the method comprising ~~the steps of~~:

~~encrypting~~ hashing the data item to generate a digest of the data item;[[,]]

~~encrypting~~ hashing each condition of the one or more conditions separately from each other and separately from the data item~~, combining the encrypted data item and the encrypted one or more conditions, and~~ to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a computer iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the ~~combination~~ last digest to generate a digital signature block that ~~inherently~~ represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature.

2-26. (Canceled)

27. (New) The method of claim 1, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

28. (New) The method of claim 1, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

29. (New) The method of claim 1, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

30. (New) The method of claim 1, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

31. (New) The method of claim 1, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

32. (New) The method of claim 1, wherein the one or more conditions consists of one condition.

33. (New) The method of claim 1, wherein the one or more conditions is a plurality of conditions.

34. (New) A computer program product, comprising a machine-readable recording medium having program code recorded thereon, said program code upon being executed by a data processing apparatus causes the data processing apparatus to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, said method comprising:

hashing the data item to generate a digest of the data item;

hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a data processing apparatus iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature.

35. (New) The computer program product of claim 34, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

36. (New) The computer program product of claim 34, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

37. (New) The computer program product of claim 34, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

38. (New) The computer program product of claim 34, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

39. (New) The computer program product of claim 34, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

40. (New) The computer program product of claim 34, wherein the one or more conditions consists of one condition.

41. (New) The computer program product of claim 34, wherein the one or more conditions is a plurality of conditions.

42. (New) A data processing apparatus comprising a computer and a machine-readable recording medium coupled to the computer, said recording medium storing program code that when executed by the computer causes the computer to perform a method for generating a conditional electronic signature, performed in response to one or more conditions being specified for an electronic signature of a data item, said method comprising:

hashing the data item to generate a digest of the data item;

hashing each condition of the one or more conditions separately from each other and separately from the data item to generate one or more condition digests respectively corresponding to the one or more conditions;

setting a reference digest equal to the digest of the data item;

a data processing apparatus iteratively processing a unique condition digest of the one or more condition digests in each iteration of a loop for a sufficient number of iterations to process all of said condition digests, said processing in each iteration comprising concatenating the reference digest with the unique condition digest of the iteration to generate a concatenand and hashing the concatenand to generate a hashed concatenand that serves as the reference digest for the next iteration if the next iteration is performed, each unique condition digest being a different

condition digest in each iteration of the loop, the regenerated reference digest of the last iteration of the loop being a last digest; and

encrypting the last digest to generate a digital signature block that represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions, said encrypting comprising signing the last digest with a digital signature.

43. (New) The data processing apparatus of claim 42, wherein said signing is performed by a signer and represents acceptance of the data item by the signer subject to the one or more conditions.

44. (New) The data processing apparatus of claim 42, wherein said signing is performed by a signer and represents acceptance of the data item by the signer, and wherein said acceptance is not subject to the one or more conditions.

45. (New) The data processing apparatus of claim 42, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block, the data item, and the one or more conditions; and

sending the communication across a network to a recipient.

46. (New) The data processing apparatus of claim 42, said method further comprising:

generating a communication, wherein the communication comprises the digital signature block and does not comprise the data item and does not comprise the one or more conditions; and

sending the communication across a network to a recipient.

47. (New) The data processing apparatus of claim 42, wherein the method further comprises:

hashing a new condition to generate a digest of the new condition;

concatenating the digital signature block with the digest of the new condition to generate a new digest;

hashing the new digest to generate a hashed new digest; and

encrypting the hashed new digest to generate a new digital signature block that represents the data item, the one or more conditions, and the new condition and enables cryptographic verification of the data item, the one or more conditions, and the new condition.

48. (New) The data processing apparatus of claim 42, wherein the one or more conditions consists of one condition.

49. (New) The data processing apparatus of claim 42, wherein the one or more conditions is a plurality of conditions.